ACEEE

Proc. of Int. Conf. on Advances in Computer Science, AETACS

A Survey on Crypto Currencies

ShaikShakeel Ahamad[1], Madhusoodhnan Nair[2]and Biju Varghese[1]
[1]eMudhra, 3rd Floor, Sai Arcade, Devarabisanahalli, Marathahalli Outer ring road, Bangalore 560103.
[2]K.G.Reddy College of Engineering and Technology, Chilkur Village, MoinabadMandal, Ranga Reddy District-501504, India, ahamadss786@gmail.com, principal@kgr.ac.in, biju.varghese@emudhra.com

***Abstract*—The world of Fiat currencies are old, outdated, not enough hard currency money supply and mismanaged by its current governments (Currency Wars) and now starting to cause Social unrest, this is only the beginning and trying to get ahead of and prevent this very serious situation from getting really out of hand. The world has experienced Global Financial Crisis (2008 -2013), Central Banks disorder = Major Social disorder & unrest. In this paper, we present a survey on crypto currencies, merits of crypto currencies compared to fiat currencies and we then compare different crypto currencies that are proposed in the literature. Finally, we propose different requirements that should be satisfied by crypto currencies to replace Fiat Currencies.**

***Index Terms*—Fiat currencies, Currency Wars, crypto currencies, Central Banks disorder, Social disorder, Global Financial Crisis**

I. INTRODUCTION

The world Fiat currencies are old, outdated, not enough hard currency money supply and mismanaged by its current governments (Currency Wars) and now starting to cause Social unrest, this is only the begging and trying to get ahead of and prevent this very serious situation from getting really out of hand. 2008 -2013 Global Financial Crisis, Central Banks disorder = Major Social disorder & unrest. You do not want to even imagine a Major case in point Financial/Currency Social disorder and unrest. Since 2008 Cyrpto Currencies are emerging and trying to make strides for a Digital Currency and Digital Currency Management System (DCMS). Currently Online merchants have been handicapped by Expensive credit card companies, High fees from escrow services, Merchant services that block many countries, complicated payment software implementation and Charge backs. There are many advantages for online merchants to using Crypto Currencies they are Monetize new markets, Lower transaction fees, Transactions reflect instantly, No charge backs and Secure. With a total Market Cap of over $1 Billion and growing the Crypto Currency economy is reminiscent of other related protocols that allowed for explosive growth through distributed networks. The Crypto Currency protocol allows for a secure digital transaction to take place over the Internet, bypassing the need to trust any third party, therefore lowering overhead cost, and providing for instant delivery of digital product for digital coins in return. Crypto Currencies is a type of digital currency which relies on cryptography, usually alongside a proof-of-work scheme, in order to create and manage the currency. A decentralized network of peer-to-peer computer nodes working in sync creates and verifies transactions of transfer of said currency within the network. Over the past few years Crypto Currencies have been shown as an Emerging Payment Systems. These new systems have been adopted by individuals and business wishing to transact quickly and efficiently over the internet without the need to supply Credit Cards or Banking information. By utilizing the characteristics of these currencies Merchants are able to setup an account and accept payments within minutes allowing customers from all over the world to purchase goods and services

DOI: 02.AETACS.2013.4.131

across borders. The nature of this currencies provide a built in mechanism where a Trust between Seller and Buyer can be established without the need for a third party to act as an escrow, therefore lowering the cost of transfer for the Buyer and risk of fraud for the Seller; as these transfers are irreversible. These Crypto Currencies are not controlled by any central entity and are not subject to any local jurisdiction, and therefore are able to transact freely across borders without the need of any due diligence preformed by any entity in order to approve or reject anyone from using said Crypto Currency. E-commerce sales topped $1 Trillion for the first time in 2012, and will continue to show double digit increase year over year for the next decade. But despite of this ever increasing industry the options for receiving and sending payment for goods and services purchased on line have not evolve to meet the needs of this global industry. A Merchant in Brazil wishing to accept payment for any goods or services rendered needs to establish a merchant account with a third party provider that will grant him/her. the ability to charge his customers. His customers must also register with the third part provider to obtain a way to pay for said products or services. Although services such as Visa, MasterCard and PayPal exist in the marketplace; they are not suitable for many Merchant or Buyer located anywhere in the world. As many Merchants and Consumers do not have established Banking systems in place and therefore do not qualify for a Credit Card or a PayPal account. The high cost and fraud associated with accepting payments via Credit Cards or PayPal online discourages many merchants and buyers from using these services. Crypto Currencies offer a secure low cost fast solution that provides an account to anyone, anywhere, anytime. A typical transaction of funds between two Crypto Currencies accounts cost less than $0.05 regardless of the amount being transferred. So if you decide to transfer $1,000.00 internationally via a Credit Card online to a Merchant, the cost to the Merchant will be approximately 3% or $30. PayPal will charge approximately 3.9% or $39. The cost through a Crypto Currency is still only $0.05 or less. And the funds transferred by a Crypto Currency account to the Merchant will not be subject to any chargeback or fraud.

II. Crypto Curriencies

Cryptocurrencies are physical precomputed files utilizing a public key / private key pairs generated around a specific encryption algorithm. The key assigns ownership of each key pair, or 'coin,' to the person who is in possession of the private key. These key pairs are stored in a file named 'wallet.dat,' which resides in a default hidden directory on the owners hard drive. The private keys are sent to users using dynamic wallet addresses generated by the users engaged in transactions. The destination payment address is the public key of the cryptocurrencykeypair. There is a finite amount of each cryptocoin available on the network, and value of each unit is assigned based on supply and demand, as well as the fluctuating difficulty levels required for mining each coin. The wallet.dat file is the most important file of the cryptocurrency software architecture, as that is where the physical cryptographic private key file is stored. Much like cash, if a user loses their wallet.dat file, or has it stolen, the cryptocurrency is lost. The decentralized nature of open source protocol ensures that the control of the network remains in the hands of the users. Transactions are dependent on participants in the network, and the user responsible for the security of their own finances and data, without the need for reliance on third parties such as banking institutions. Bitcoin operates as a p2p file sharing protocol, and therefore the concept is similar to .torrent technology. The p2p network relies on user participation for successful trusted data exchange. Each transaction is confirmed through key verification on multiple nodes in the network before reaching its destination. This crowdsourced key verification process guarantees the integrity of the data transfer. The most popular cryptocurrency at the time of writing is Bitcoin, with alternatives such as Litecoin rapidly gaining market traction. The source code for these programs, as well as the code for other cryptocurrencies, are available on all major open source code repositories.

III. Types of Cryptocurrency

A. Bitcoin

The first cryptocurrency to emerge was Bitcoin (BTC), based on the SHA-256 algorithm. This virtual commodity was conceptualized in a whitepaper written in 2009 by a pseudonymous author who went by the name Satoshi Nakamoto. Over the course Bitcoin's first four years, the market price of a single Bitcoin has fluctuated from below $0.01USD to over $250USD. The highly volatile price has made Bitcoin an attractive investment alternative for traders seeking to profit from market speculation, while at the same time the

market volatility has made long term investors and daily users hesitant to participate for long periods of time. A single Bitcoin can be spent in fractional increments that can be as small as 0.00000001 BTC per transaction. The smallest increment of a Bitcoin is known as a Satoshi, named after the original whitepaper author. The protocol allows for incremental transactions in the event the value of BTC to rises to the point where micro transactions will become commonplace. The rise in the value of BTC is anticipated because there is a limit to the total amount of Bitcoin will ever be created. Once the Bitcoinblockchain is completed, users can only circulate the coin that still exists on the network. As time goes on, Bitcoin will be lost and destroyed through daily use. The principles of supply and demand economics will come into play, increasing value of remaining Bitcoin. Bitcoin is currently the most reputable of all cryptocurrency, as it is the oldest, and has been the subject of mainstream media coverage due to rapid market fluctuations and an innovative technical concept. At the time of writing, Bitcoin can be interpreted as being the 'gold standard' of cryptocurrency because all alternative cryptocurrency market prices are matched to the price of BTC.

B. Litecoin [3]

Litecoin (LTC) can be considered the 'silver standard' of cryptocurrency, as it has been the second most adopted cryptocurrency by both miners and exchanges. Litecoin makes use of the Scrypt encryption algorithm, as opposed to SHA-256. One of the goals of Litecoin was to have transactions confirm at a faster speed than on the Bitcoin network, as well as make use of an algorithm that was resistant to accelerated hardware mining technologies such as ASIC. At the time of writing, the Scrypt algorithm is resistant to ASIC mining due to intense RAM requirements. The total amount of Litecoin that is available for mining and circulation is four times the amount of Bitcoin, meaning there will be quadruple the amount of Litecoin available to Bitcoin [3].

C. Altcoins

'Altcoin' a is slang term for the dozens of project forks that have emerged within the cryptocurrency software development community. Altcoins are 'forks' of either Bitcoin or Litecoin, meaning they make use of SHA-256 or Scrypt encryption algorithms and feature their own unique properties. Names of various altcoins range from memorable to comical (Feathercoin, Terracoin, P2PCoin, BitBar, ChinaCoin, BBQCoin). The profitability of mining and trading altcoin varies on a daily basis. Some altcoins exceed the profitability of Bitcoin at times, while others are less profitable. It is believed by some cryptoeconomists that altcoins contribute to a diverse cryptocommodities marketplace, which is a good thing as there is more opportunity for speculative arbitrage and mining difficulty levels are spread over many different networks. Other cryptoeconomists disagree about the beneficial aspects of altcoins, citing overuse of the cryptocoin concept will dilute widespread adoption and restrict the use of the technology to speculative trade markets instead of daily commerce.

D. Other Coins

These coins are „forks" of either Bitcoin [1, 2] or Litecoin, meaning they make use of SHA-256 or Scrypt encryption algorithms and feature their own unique properties. Names of various altcoins range from memorable to comical (Feathercoin, Terracoin, P2PCoin, BitBar, ChinaCoin, BBQCoin). The profitability of mining and trading altcoin varies on a daily basis. Some altcoins exceed the profitability of Bitcoin at times, while others are less profitable. It is believed by some cryptoeconomists that altcoins contribute to a diverse cryptocommodities marketplace, which is a good thing as there is more opportunity for speculative arbitrage and mining difficulty levels are spread over many different networks. Other cryptoeconomists disagree about the beneficial aspects of altcoins, citing overuse of the cryptocoin concept will dilute widespread adoption and restrict the use of the technology to speculative trade markets instead of daily commerce.

E. Mining Cryptocurrency

The term 'mining' is slang for the use of computational power to process transactions for a cryptocurrencyblockchain in order to receive a reward of cryptocurrency for the effort. The computational power will come in the form of CPU processing or GPU processing. Miners are rewarded for successful 'shares,' or completed computations, by receiving a payment with fees that are collected along the way by the p2p network. At the time of writing, the reward for a successfully completed Bitcoin block is 25 BTC and 50 LTC for a Litecoin block, and diminishes as the blockchain grows. The computational power requirements differ depending on the encryption algorithm being used. SHA-256 mining rates are measured in GH/s, whereas Scrypt mining rates are measured in KH/s. While the Crypto Currency transaction from one

account holder to another is very smooth, fast and efficient, the conversion between Fiat Currency to Crypto Currency has proven difficult for the masses and has kept many Merchants, Customers, Traders and Investors from joining this new revolutionary way to transfer funds across the globe with a quick and easy click of the mouse. There are a few ways one is able to obtain Crypto Currencies; these are very "simple" explanations: By Mining it, which simply put without getting too technical means that any CPU (Central Processing Unit), a GPU (Graphic Processing Unit) or the more advanced ASIC (Application Specific Integrated Circuit) can be used to connect to the Crypto Currency network and participate in the Verification and Confirmation process of a Crypto Currency transaction. By doing so, the transfer fees and newly minted currency are bundled and automatically transferred to the application that was able to provide a solution to a specific block of transactions. The same way the Visa network approves charges, the Crypto Currency network helps approve transactions. Since the network has expanded exponentially over the past year, mining has become less profitable for the average miner. Mining new blocks result in an average of more than $400,000 in new Currency created every day, which help incentives miners to continue supporting the network. By Selling Goods and Services for Crypto Currencies; many merchants are choosing to accept Crypto Currencies in return for selling Goods and Services. By Exchanging Fiat Currency to Crypto Currencies, the most popular way for one to obtain Crypto Currencies is to purchase them for exchange for Fiat Currencies. We at Crypto Financial believe that e-commerce needs a fast pace moving currency to match today's global need for speed. A currency for the Internet; and we believe that in the not so distant future Crypto Currencies will prove to be the leaders to become the World Wide Web standard for trade. We aim to change the status quo and provide a new way for Merchants, Customers, Traders and Investors the ability to interact with one another instantly and efficiently, by providing them with the ability to convert their Fiat to Crypto Currency and *vice versa* via our Financial Services Solutions.

IV. Our Proposed Digital Currency

Our proposed crypto currency (crypcurr) satisfies all the above requirements **by a**dopting Application Specific Integrated Circuits (ASIC) mining for our proposed CrypCurr (Crypt Currency) for getting more computational processing power using significantly less resources than GPU mining such as hardware and electricity. Our proposed "CrypCurr" should overcome the following common attacks against Cryptocurrency such as Data Breaches of Mining Pools/Trading Platforms/Third Party Wallet Storage. There are pros and cons to both sides of the currency debate. Crypto-currency (such as Bit coin) does not provide the same level of fraud protection, among other protections, that a fiat currency controlled by banks has traditionally offered. Fiat currencies are problematic because they are not efficient, are prone to theft and counterfeiting, and are vulnerable to political swings. We envisage that future is with cryptographically implemented fiat currencies it will be a bottom-up movement. A fiat-based crypto-currency could operate alongside these other services as an alternative technology-based mechanism for money transmission. The liabilities—like those held by most banks, credit card companies, and money transmission services—would fall squarely on the companies providing the software to use the crypto-currency. There are a few regulations that the new crypto-currency providers would need to observe, but it is nothing outside the realm of what normal money transmission services must follow today. Over time, technical bugs or issues found with the crypto-currency will be resolved. As trust in fiat-based crypto-currencies grows, we will see greater pressure applied to traditional banking and money transmission services due to the efficiency gains identified through the use of crypto-currencies. Developing nations may be the first to make the switch since they are not politically influenced by the banking and finance sector to the degree that more developed nations are. Other nations may choose to adopt crypto-currencies in order to increase the efficiency of their market, thus giving them a competitive advantage. Ultimately, the path to a crypto-currency will not be a proprietary one. Proprietary solutions have never seen the type of acceptance that results in long-term societal adoption. To replace cash, it is necessary to have an open crypto-currency standard. Specifications for operating an open crypto-currency network must be published just as the World Wide Web Consortium published specifications for operating an open Web. For a technology to become ubiquitous, it must first be published as a patent and royalty-free specification. Fiat currencies are problematic because they are not efficient, Centralized, are prone to theft and counterfeiting, and are vulnerable to political swings. Our proposed fiat-based crypto-currency could operate alongside these other services as an alternative technology-based mechanism for money transmission and overcomes all the limitations of Fiat currencies. Following are the requirements that need to be satisfied for a new crypto-currency protocol to be successful.

a) It has all of the benefits of cash.

b) Unlike cash, it is highly resistant to theft and counterfeiting.
c) It should ensure pseudo anonymity
d) *Open protocol:* How the money is created, exchanged, and destroyed by the currency network must be published as an open protocol.
e) *Anonymous:* Your identity should be protected when transacting with a digital bill. When you transfer an amount from yourself to someone else, the transaction should not be traced back to you without your consent.
f) *Extremely counterfeit-resistant:* The ability to illegally mint new money must be as close to impossible as the current technology allows.
g) *Protection from theft:* Therefore, it is imperative that protection and recourse from theft be a core part of the design of such a system.
h) *Multipoint authenticity:* The authenticity of any amount in circulation must be verifiable through at least two independent mechanisms.
i) *Efficient:* The operation of a digital currency should be highly efficient without requiring a great deal of processing overhead. By removing the need to physically handle cash, and publicly and anonymously storing the global transaction log on the Web (using trusted and robust cryptographic methods), we can maximize the efficiency of a crypto-currency and keep operational costs to a minimum.
j) *Resilient:* Ideally, a digital currency network should be resilient in the face of multiple system failures. The Web provides a great model for this sort of resiliency through decentralization. That is not to say that fully decentralized currency systems are perfect, as protection against theft is very difficult to achieve in such systems. However, a balance can be achieved to reasonably ensure that the currency network is not so centralized that the currency is useless if a central checkpointing mechanism goes down for a week or more.
k) It should overcome"blockchain bloat" problem

CrypCurr: Designing aCrypCurr (our proposed) Protocol which overcomes the limitations of the existing solutions such as Bitcoin, Litecoin, Namecoin, PPcoin, Terracoin and Devcoin

CrypCurrJ: A CrypCurrJ is a Java implementation of the CrypCurr protocol, which allows it to maintain a wallet and send/receive transactions without needing a local copy of the official implementation. It is suitable for using on constrained devices such as mobile phones or cheap virtual servers.

CrypCurrW: With this app you always have your wallet in your mobile phone. You can send payments simply by scanning a QR-code, by bluettoth and by touching two phones together (NFC). CrypCurrW Wallet is designed to be easy to use, reliable, secure and fast. Display of wallet balance. Sending and receiving of CrypCurr via NFC, QR-codes or by Bluetooth. Enter transactions while offline, will be executed when online. Manages blockchain on your device (for enhanced security).

XChange: XChange is a library providing a simple and consistent API for interacting with a diverse set of financial security exchanges.

CrypCurrM: CrypCurrM is a complete online merchant platform designed for use with CrypCurr an internet currency that has many unique features.

V. Data Breaches of Mining Pools/Trading Platforms/Third Party Wallet Storage

Many cryptocurrency web applications are often based on experimental concepts that may have undisclosed vulnerabilities. Furthermore, many also rely on the end user to set a secure password. As with any security control, it is only as strong as it's weakest link. Malicious actors have been known to attack web applications that manage cryptocurrency wallets, as well as attack users who have reused breached passwords and/or experienced compromised e-mail accounts and password resets. Major mining pools and exchanges have implemented PIN solutions, two factor authentication, and CAPTCHAs to prevent such activity. However many smaller mining pools are still experiencing the growing pains associated with the implementation of new technologies, such as APIs, and are victim to pool heists. As e-commerce merchants start accepting Bitcoin, they will also be targets of such attacks and should prepare through proper web application vulnerability analysis and end user education.

VI. Attacks Against The End User

Client Side Attacks -Since Bitcoin and other cryptocurrency resides in the wallet.dat file, a goal of malicious actors in a cryptocurrency attack campaign is the exfiltration of that file. This can be achieved through physical access, but is most often attributed to malware. Both whitehat and blackhat tools exist for the theft of Bitcoin wallets. The tool was developed and released by hacker iLLwiLL of the hacking group iLLmoB. The Bitcoin wallet stealer Metasploit post exploitation module was released shortly after Bitcoin's

VII. Government Seizure As Contraband

The first documented seizure of Bitcoin took place in June 2013. The United States Drug Enforcement Administration (DEA) seized approximately 11 Bitcoins from a suspect that was accused of illegal activities using an underground e-commerce marketplace. The seizure and the physical robbery indicates that cryptocurrencies have solidified themselves as a valuable commodity to both common thieves and law enforcement agencies, demonstrating that Bitcoin and the cryptocurrency concept has longevity and will continue to gain traction with the general population.

VIII. Limits of Cryptocurrency

Like any emerging technology, cryptocurrency still has a way to go before it is refined and perfected as a commodity suitable for daily commercial use by the average person.

A. Blockchain Size

Large public blockchain makes for slow setup of Bitcoin wallets and requires large storage space. As of the time of writing, the Bitcoinblockchain is over 8GB in size. This blockchain size can be problematic with mobile devices, and as the blockchain grows 3rd party storage solutions may become only option. The reliance on a third party storage solution would defeats the purpose of the principles of being in control of commodity, and subject users to the regulations and terms of service of the solution provider.

B. Privacy

The public blockchain of cryptocurrencies documents payment address, IP address, and all incoming/outgoing transactions to that address. If anonymity practices are not followed, such as the use of a VPN or the Tor network, then the transaction is attributable in a way that is more public and verifiable than a credit card or cash. This attribution is made even easier if at some point in time the end user has documented their real name along with a Bitcoin payment address.

IX. Technical Barriers

It's hard enough helping the average person navigate simple IT issues. In addition to standard computer navigation, the end user has to understand the concepts of public key private key encryption, peer to peer protocols, mining share submissions, blockchains, and market fluctuations due to supply/demand commodity trading economics. Once those concepts are clear to the end user, only then will they feel totally confident buying and selling on the internet using cryptocurrency. As with any organized criminal, the target will be the location of money. In the case of cryptocurrencies, the locations of value are in the form of mining pool servers, trading platforms, third party wallet services, and end user computers. Over the short history of cryptocurrency, each value location has experienced multiple forms of attack that resulted in the direct theft of coins.

X. Asic Mining

Application Specific Integrated Circuits (ASIC) have been developed for Bitcoin. Due to the customized and specific nature of ASIC technology, there is currently only ASIC for Bitcoin. ASIC mining is advertised as having exponentially more computational processing power using significantly less resources than GPU mining, such as hardware and electricity. It is hypothesized that as the popularity of ASIC accelerated hardware grows among the Bitcoin mining community, GPU miners will begin switching to Litecoin or other altcoins that are resistant to ASIC technologies. The benefits and drawbacks of this type of diversification is currently a popular subject of debate among the mining community.

XI. Conclusion

Fiat currencies are old, outdated, not enough hard currency money supply and mismanaged by its current governments (Currency Wars) and now starting to cause Social unrest, this is only the beginning and trying to get ahead of and prevent this very serious situation from getting really out of hand. The world has experienced Global Financial Crisis (2008 -2013), Central Banks disorder = Major Social disorder & unrest.In this paper, we present a survey on crypto currencies, merits of crypto currencies compared to fiat currencies and we then compare different crypto currencies that are proposed in the literature. Finally, we propose different requirements that should be satisfied by crypto currencies to replace Fiat Currencies.

References

[1] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," Tech. Rep., 2011.[Online]. Available: http://arxiv.org/abs/1107.4524

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf

[3] Litecoin into the future – Litecoin crypto currency. http://litecointrader.com/Litecoin-Future.html